U.S. Department of Justice
Federal Bureau of Investigation

November 2011

FBI Law Enforcement Bulletin

Cyber Terror

November 2011
Volume 80
Number 11

**United States
Department of Justice
Federal Bureau of Investigation
Washington, DC 20535-0001**

**Robert S. Mueller III
Director**

Contributors' opinions and statements should not be considered an endorsement by the FBI for any policy, program, or service.

The attorney general has determined that the publication of this periodical is necessary in the transaction of the public business required by law. Use of funds for printing this periodical has been approved by the director of the Office of Management and Budget.

The *FBI Law Enforcement Bulletin* (ISSN-0014-5688) is published monthly by the Federal Bureau of Investigation, 935 Pennsylvania Avenue, N.W., Washington, D.C. 20535-0001. Periodicals postage paid at Washington, D.C., and additional mailing offices. Postmaster: Send address changes to Editor, *FBI Law Enforcement Bulletin*, FBI Academy, Quantico, VA 22135.

The Training Division's Outreach and Communications Unit produces this publication with assistance from the division's National Academy Unit. Issues are available online at *http://www.fbi.gov*.

E-mail Address
leb@fbiacademy.edu

Cover Photo
© shutterstock.com

Send article submissions to Editor, *FBI Law Enforcement Bulletin*, FBI Academy, Quantico, VA 22135.

FBI Law Enforcement Bulletin

Features

Departments

ISSN 0014-5688 USPS 383-310

Cyber Terror

By WILLIAM L. TAFOYA, Ph.D.

Anyone ever misquoted recognizes the importance of context. Wrong assumptions about concepts, words, and phrases easily lead to misunderstanding. In the law enforcement community, officers who use a weapon in the line of duty to defend themselves or innocent bystanders may kill but not murder. Context often serves as the crucial variable justifying the use of deadly force. Murder is always killing, but killing is not always murder. Similarly, accurate knowledge of the context and targets of cyber attacks enhances clarity and helps to avoid obscuring intent.

"Cyber terrorism is a component of information warfare, but information warfare is not... cyber terrorism. For this reason, it is necessary to define these topics as separate entities."[1] Said another way, undefined and misunderstood terms easily could lead a conversation to proceed along parallel lines rather than an intersecting track. Thus, differentiating concepts and terms is important, as in the case of understanding what cyber terror is and what it is not.

INFORMATION WARFARE

Dorothy Denning, one often-cited expert, describes but does not define information warfare (IW): "Information warfare consists of offensive and defensive operations against information resources of a 'win-lose' nature."

Further, "Information warfare is about operations that target or exploit information resources."[2] Nevertheless, several secondary and tertiary sources term her description "Denning's Definition."[3] Other researchers assert that "Information warfare is combat operations in a high-tech battlefield environment in which both sides use information technology means, equipment, or systems in a rivalry over the power to obtain, control, and use information."[4]

IW has several variants. Electronic warfare (EW), primarily a military term, is older than IW and dates back to World War II. Information operations (IO) is the more contemporary military nomenclature. EW and IO both are synonymous with IW. None of the three, however, are synonymous with cyber terror. IW, EW, and IO encompass the use of cryptography (cryptology and cryptanalysis), radar jamming, high-altitude aerial reconnaissance, electronic surveillance, electronically acquired intelligence, and steganography. Cyber terrorists may use these same tools. The distinction, however, is not the technological tools employed but the context and target.

In 1991 during Operation Desert Storm, coalition forces used IW, EW, and IO through the clandestine introduction of viruses and logic bombs into Iraqi Republican Guard (IRG) command-and-control-center computers and peripherals, causing the disruption and alteration of the targeting and launching of Scud missiles.[5] Military combatants engaging one another on the battlefield constitutes IW, EO, and IO. Attacking the largely civilian critical infrastructure is not warfare, but terrorism—cyber terror. But, how does cyber terror differ from IW, EW, and IO?

"Clearly, law enforcement agencies need to stay well informed about what the experts think."

Dr. Tafoya, a retired FBI special agent, is the coordinator of and a professor in the Information Protection and Security Program at the University of New Haven in Connecticut.

CYBER TERROR

The term was coined in the 1980s by Barry Collin who discussed this dynamic of terrorism as transcendence from the physical to the virtual realm and "the intersection, the convergence of these two worlds...."[6] The Center for Strategic and International Studies (CSIS) has defined it as "the use of computer network tools to shut down critical national infrastructures (e.g., energy, transportation, government operations) or to coerce or intimidate a government or civilian population."[7] The author defines *cyber terror* as "the intimidation of civilian enterprise through the use of high technology to bring about political, religious, or ideological aims, actions that result in disabling or deleting critical infrastructure data or information."

As an illustration in size, this article does not compare to the holdings of the Library of Congress. The loss of the former would be traumatic to the author, but would impact few other people. Loss of the

latter, likely irreplaceable, would prove devastating if a cyber attack deleted those files. Of course, neither could compare to the loss of one human life. But, if data or information from any of the nation's critical infrastructure databases were attacked and destroyed, that certainly would impact quality of life.

One expert asserted that if people wanted to know how much to spend on information security, they should calculate the cost of replacing their hard drives and databases in the event they became intentionally wiped out—then, double that estimate.[8] Recently, a graduate student observed that "Cyber terrorism is a critical threat to national security and public policy. The intelligence community (IC) is at a turning point because it is difficult to catch a criminal who establishes an identity in cyberspace. Further, [we are at] a critical point in [time] for public policy because the government will have to devise regulations of electronic data transfer for public, as well as private, information that can be identified and accessed via the Internet."[9]

Although some experts assert that no credible evidence exists that terrorists have initiated cyber attacks, groups, such as Hamas and Hezbollah, allegedly undertook such attacks more than a decade ago.[10] "Lone wolves" have perpetrated more recent ones. The highest levels of government have emphasized the need to focus on this specter.[11]

What are the most vulnerable targets of cyber terrorists? What constitutes the significance of the targets and the magnitude of the threat? Does it matter what the threat is called? Does cyber terror constitute an element of computer crime?

> ***…where do vulnerabilities lie, and what technological tools will terrorists use?***

COMPUTER CRIME

More than a half century later, not even the most prominent authorities have reached a consensus about what constitutes computer crime. According to one of the pioneers of this genre, the earliest occurrence of such abuse occurred in 1958.[12] The first prosecution under federal law, the Computer Fraud and Abuse Act, Title 18, Section 1030, U.S. Code, was of Robert Tappan Morris, Jr., then a graduate student of computer science, who unleashed the so-called Internet Worm in 1988.[13]

Along the time continuum, this is where the line begins to blur between "conventional" computer crime and what the author refers to as cyber terror. This genus includes the Melissa Virus (1999), ILOVEYOU Virus (2001), Code Red Worm (2002), Blaster Virus (2004), and Conficker Worm (2008). These attacks differ from extortion, fraud, identify theft, and various scams, all of which certainly are malicious. However, acts of cyber terror *as here defined* impact society—even the nation—not just an individual, elements of the business sector, or government agencies.

Space limitations do not allow for an incident-by-incident accounting of cyber terror episodes. One example is the case of *U.S. v. Mitra*. In 2003, Rajib K. Mitra undertook an ongoing attack on a police emergency radio system. Initially, authorities investigated Mitra's cyber assaults as a violation of Wisconsin state law, but, ultimately, deemed them attacks on the critical infrastructure. The case was prosecuted under federal law (Computer Fraud and Abuse Act). Mitra, a lone wolf, was tried and convicted on March 12, 2004, and later sentenced to 96 months imprisonment. Subsequently, his appeal failed. U.S. Seventh Circuit Court of Appeals judges

ruled unanimously, noting that "it is impossible to fathom why any sane person would think that the penalty for crippling an emergency-communication system on which lives may depend should [not] be higher than the penalty for hacking into a Web site to leave a rude message."[14]

Clearly, law enforcement agencies need to stay well informed about what the experts think. Most contemporary professionals remain cautious. However, if people wait until they have absolute proof positive, it may be too late. The cyber trends seem clear. Over the course of approximately 13 years, both the number and frequency of instances of digital disorder have intensified, and the sophistication and diversity of types of cyber attacks have increased.

One high-profile specialist contended that "stories of terrorists controlling the power grid, or opening dams, or taking over the air traffic control network and colliding airplanes, are unrealistic scare stories." He went on to invoke a cost-benefit ratio perspective: "We need to understand the actual risks. Here's the critical question we need to answer: Just how likely is a terrorist attack, and how damaging is it likely to be?"[15] Another authority notes that "threats to the critical infrastructure are becoming increasingly frequent" and goes on to say, "Cyber attacks are one of the greatest threats to international peace and security in the 21st Century."[16] Where there is smoke, is fire not obviously far behind? And, what about the future? What technological innovations will impact the ability to serve and protect in the near-term future?

TOMORROW'S CHALLENGES

Concerning the use of the term *cyber terror*, do experts resemble the proverbial blind men who feel different parts of the same elephant? On the near-term horizon, technological wonders will arise of which the unscrupulous will avail themselves, just as others before them have done.[17] But, where do vulnerabilities lie, and what technological tools will terrorists use?

SCADA Systems

Not the only concern, but certainly a major worry, are supervisory control and data acquisition (SCADA) systems. Closely related are digital control systems (DCS) and programmable logic controllers (PLC). SCADA systems are more ubiquitous than personal computers and laptops combined. Without onsite human intervention, they automatically and remotely collect data from sensors in devices used for industrial processing. They store information in databases for subsequent central-site management and processing.

SCADA systems have existed since the 1960s. In the early days, they were stand-alone, and few were networked. Today, virtually all are accessed via the Internet. This may be great as a cost-cutting measure, but not from an information security perspective. Quietly and without fanfare, SCADA systems have proliferated rapidly—for starters, in the electric, oil, and gas; water treatment; waste management; and maritime, air, railroad, and automobile traffic control industries. SCADA systems also are embedded in "telephone and cell phone networks, including 911 emergency services."[18]

These obscure little drone-like computer systems have virtually no security, firewalls, routers, or antivirus software to protect them. They are spread far and wide across the nation, even in some of the most

remote places imaginable.[19] One anonymous hacker interviewed for a television program said, "SCADA is a standard approach toward control systems that pervades everything from water supply to fuel lines." He goes on to describe that the systems run operating systems that make them vulnerable.[20]

Ominous Threats

Electromagnetic pulse (EMP) bombs and high-energy radio frequency (HERF) weapons differ from the malicious codes, computer viruses, and worms of yesteryear. While the latter remain worrisome, EMP and HERF are serious menacing perils of the near-term technological age. EMP devices are compact, and perpetrators can use them to overload computer circuitry. These devices can destroy a computer's motherboard and permanently, irretrievably erase data in memory storage devices.[21] Like EMPs, HERF devices use *electromagnetic radiation*.[22] They, too, deliver heat, mechanical, or electrical energy to a target. The difference is that individuals can focus HERF devices on a specific target using a *parabolic reflector*.[23] HERF, as asserted, does not cause permanent damage—EMP does.[24] An array of demonstrations of the power of such homemade devices is depicted at several Web sources, such as YouTube.

Bots

Two decades ago, an expert warned about Internet agents, including bots (robots), Web crawlers, Web spiders, and Web scutters, software apps that traverse the Internet while undertaking repetitive tasks, such as retrieving linked pages, specified words or phrases, or e-mail addresses.[25] Although bots have served benign functions—for example, harvesting e-mail addresses—for many years, they now loom large as a near-term future IC and policing issue. More recent research supports this contention. Given these forecasts, the question is not what might happen tomorrow, but, rather, how well-prepared law enforcement will be to protect and serve.

> ***…law enforcement agencies should be prepared to deal with the aftermath of hard-to-forecast, but not regularly reoccurring, cyber attacks on the nation's critical infrastructure.***

IMPLICATIONS FOR LAW ENFORCEMENT

Federal agencies responsible for investigating terrorism, including cyber terror, must remain vigilant. This includes ensuring adequate funding for staffing, equipment, and training. But, beyond that, local law enforcement officers must encourage citizens to be alert and to report suspicious behavior. Many local law enforcement agencies have had useful resources, such as citizens' police academies, for decades. These programs can educate taxpayers about activity in the physical realm that should be reported. However, what about transcendence to the virtual realm? Since 1996, the FBI's InfraGard Program, an information sharing and analysis effort, has focused on marshaling the talents of members of America's information security (INFOSEC) community.[26] However, what of "main street USA"?

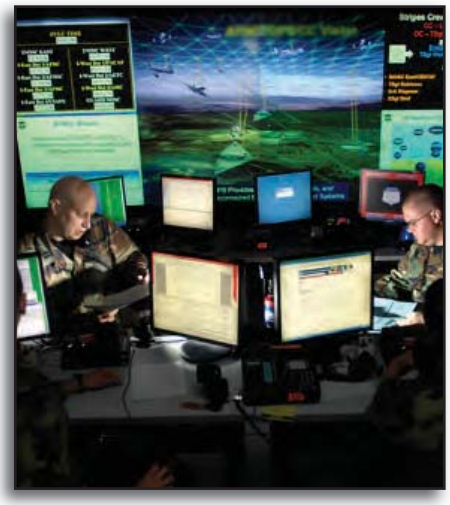
See Something, Say Something is a terrific crime prevention slogan promoted in New York City.[27] It seems to have resonated recently in Times Square when an observant man, a street vendor and Vietnam veteran, alerted the New York Police Department to the SUV used in what turned out to be, fortunately, a failed Taliban-sponsored car-bombing attempt.[28] Any such program should be augmented to provide to its participants

examples of behavior in the business community, including those in a work environment, that could alert authorities to precursors of potential cyber misdeeds. Just as someone does not need specialized education to recognize threats in real life, anyone can recognize these digital threats. One authority notes that "an example of suspicious behavior might be a bit of malicious program attempting to install itself from opening an office document." To reduce the threat, employees could add a "'behavior' layer to [antivirus products]."[29] Of course, this suggestion could unnerve many civil liberty-oriented watchdog organizations; there is no reason not to include such agencies in the discussion, planning, and implementation of the augmentation here proposed. What, then, is the bottom line?

NECESSARY PREPARATIONS

Earthquakes, hurricanes, tsunamis, tornadoes, volcanoes, toxic spills, forest fires, and shark attacks do not occur with great frequency. Precautions, nevertheless, are in place to protect people from the physical threats posed when these natural but seldom-occurring violent events occur. Although they cannot be forecast with great accuracy, we are prepared for them. Similarly, law enforcement agencies should be prepared to deal with the aftermath of hard-to-forecast, but not regularly reoccurring, cyber attacks on the nation's critical infrastructure.

Criminals are menacing our cyber shores, preparing to launch a large-scale attack. What is clear is that it will happen. What is not obvious is by whom or when. Respected



INFOSEC authorities have made a compelling case for the "swarm"—attacks via different paths by dispersed cells. Al Qaeda already has demonstrated an understanding of the technique.[30] Other countries, such as India, Saudi Arabia, China, France, Brazil, and Spain, already have experienced such attacks.[31] Additionally, well-known U.S. companies have reported major breaches targeting source code.[32]

Cyber terrorists are pinging ports and probing our digital fortifications as they endeavor to identify vulnerabilities. Daily crackers and terrorists are skulking, battering firewalls, and learning more each time they do so. Clearly, preparations to thwart such attacks are necessary.

CONCLUSION

The skills, tools, and techniques are the same, but information warfare is conducted between military combatants; cyber terrorism targets civilians. Cyber terrorists indiscriminately will attack the nation's critical infrastructure and civilians—the innocent. Thus, the context and targets, not the technological tools or frequency of attacks, are the more appropriate delimiters that distinguish cyber terror from information warfare.

Some of these criminals are being caught and prosecuted, but more remain undetected. To best serve its motto, "to protect and serve," law enforcement must proactively guard this country's national security on every front. ✦

Endnotes

[1] Robert Taylor, Eric Fritsch, Tory Caeti, Kall Loper, and John Liederbach, *Digital Crime and Digital Terrorism* (Upper Saddle River, NJ: Pearson Prentice Hall, 2011), 19.

[2] Dorothy Denning, *Information Warfare and Security* (Reading, MA: Addison-Wesley Longman, 1999), 21.

[3] Maura Conway, "Cyberterrorism: Hype and Reality," in *Information*

Warfare: Separating Hype from Reality, ed. E. Leigh Armistead (Washington, DC: Potomac Books, 2007), 73–93.

[4] Wang Baocun and Li Fei, "Information Warfare," Academy of Military Science, Beijing, China, *http://www.fas.org/irp/world/china/docs/iw_wang.htm* (accessed October 28, 2010).

[5] Denning; and Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston, MA: Little, Brown, 1993).

[6] Barry Collin, "The Future of Cyberterrorism," *Crime & Justice International Journal* (March 1997): 15.

[7] James Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," Center for Strategic and International Studies, *http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf* (accessed October 28, 2010).

[8] Dr. Grace Hopper, "Future of Computing" (lectures, FBI Academy, Quantico, VA, 1985-1991). See also *http://www.sdsc.edu/ScienceWomen/hopper.html* (accessed October 29, 2010); *http://www.youtube.com/watch?v=7sUT7gFQEsY* (accessed October 29, 2010); and *http://www.youtube.com/watch?v=CVMhPVInxoE&feature=related* (accessed October 29, 2010).

[9] Mehwish Salim, "Cyber Terror: Unequivocal Threat or Hyperbole?" (award-winning paper presentation, 34th Annual Meeting of the Northeastern Association of Criminal Justice Sciences, Bristol, RI, June 9-12, 2010).

[10] David Pettinari, "Cyber Terrorism-Information Warfare in Every Hamlet," *Police Futurist* 5, no. 3 (1997): 7-8.

[11] National Security Council, "The Comprehensive National Cybersecurity Initiative," *http://www.globalsecurity.org/security/library/policy/national/cnci_2010.htm* (accessed October 29, 2010); and CBS, "Sabotaging the System," *60 Minutes*, *http://video.techrepublic.com.com/2422-13792_11-364499.html* (accessed October 29 2010).

[12] Donn Parker, *Crime by Computer* (New York, NY: Charles Scribner's Sons, 1976).

[13] Ronald Standler, "Computer Crime," *http://www.rbs2.com/ccrime.htm* (accessed October 29, 2010).

[14] *U.S. v. Mitra* 04-2328.

[15] Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (New York, NY: Copernicus Books, 2003).

[16] Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA: O'Reilly, 2010).

[17] For more information, visit *http://www.battelle.org*.

[18] Gregory Coates, "Collaborative, Trust-Based Security Mechanisms for a National Utility Intranet" (master's thesis, Air Force Institute of Technology, 2007).

> ***…officers must encourage citizens to be alert and to report suspicious behavior.***

[19] William Graham, Chairman, Critical National Infrastructures, "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack," EMP Commission, *http://empcommission.org/docs/A2473-EMP_Commission-7MB.pdf* (accessed October 29, 2010); Seth Fogie, "SCADA and Security," *http://www.informit.com/guides/content.aspx?g=security&seqNum=322* (accessed October 29, 2010); and Seth Fogie, "SCADA In-Security," *http://www.informit.com/guides/content.aspx?g=security&seqNum=323* (accessed October 29, 2010).

[20] Tom Longstaff, "Cyberwar: Vulnerability of Scada Systems?" *http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/vulnerable/scada.html* (accessed October 29, 2010).

[21] Graham.

[22] For additional information, see *http://www.lbl.gov/MicroWorlds/ALSTool/EMSpec/* (accessed October 29, 2010).

[23] For additional information, see *http://www.wordiq.com/definition/Parabolic_reflector* (accessed October 29, 2010).

[24] John Geis, "Directed Energy Weapons of the Battlefield: A New Vision for 2025" (paper, Center for Strategy and Technology, Air War University, Maxwell Air Force Base, Alabama, 2003).

[25] Kevin Manson, "Robots, Wanderers, Spiders and Avatars: The Virtual Investigator and Community Policing Behind the Thin Digital Blue Line" (presentation, annual meeting of the Academy of Criminal Justice Sciences, Louisville, KY, March 15, 1997).

[26] For more information, visit *http://www.infragard.net.*

[27] For more information, visit *http://www.mta.info/mta/security/index.html.*

[28] "President Calls to Thank Times Square Vendor," *Associated Press*, May 2, 2010; and Anne Komblut,"Pakistani Taliban Behind Attempted Times Square Car Bombing, Attorney General Says," *Washington Post*, May 9, 2010.

[29] Frances Alonzo, "Security Expert Urges Shift in Tactics Against Cyber Attacks," *http://it.moldova.org/news/security-expert-urges-shift-in-tactics-against-cyber-attacks-206747-eng.html* (accessed October 29, 2010).

[30] John Arquilla and David Ronfeldt, *Swarming and the Future of Conflict* (Santa Monica, CA: RAND, 2000); and John Arquilla and David Ronfeldt, "Fighting the Network War," *Wired* 9, no. 12 (2001).

[31] Kim Zetter, "Google Hackers Targeted Source Code of More Than 30 Companies," *http://www.wired.com/threatlevel/2010/01/google-hack-attack/* (accessed October 29, 2010).

[32] Kim Zetter, "Report: Critical Infrastructures Under Constant Cyberattack Globally" *http://www.wired.com/threatlevel/2010/01/csis-report-on-cybersecurity/* (accessed October 29, 2010).

Crimes Against Children Spotlight

Child Abduction Rapid Deployment (CARD) Team

By Ashli-Jade Douglas

"One missing child is too many. At the FBI, saving lives, protecting the innocent, and hunting down those who prey upon them is at the heart of what we do…. Protecting our children is one priority where our commitment is stronger than ever."

—FBI Director Robert S. Mueller, III

FBI research revealed that 74 percent of children abducted and murdered were killed within the first 3 hours of their disappearance. To aid local law enforcement and FBI investigators in child abduction investigations, the FBI created the Child Abduction Rapid Deployment (CARD) team in 2006. Since its inception, CARD has provided field offices with the resource of additional investigators with specialized experience in child abduction matters. As of September 2011, the CARD team has assisted in the investigation of 69 child abduction cases involving 77 children. Of the 77 children, 31 were recovered alive; 11 remain missing. CARD statistics also indicated that in 70 percent of these cases, the child was abducted by an individual with a known relationship to the child. In contrast, 10 percent of abductors were registered sex offenders.

A total of 60 CARD team members are divided into 10 separate groups, 2 within each region of the United States, representing the Northeast, Southeast, North Central, South Central, and Western parts of the country. Regionally, CARD provides rapid, on-site response, including investigative, technical, and resource assistance, during the most critical time period following a child abduction.

CARD has the unique experience of having investigated many child abduction cases, whereas a

majority of seasoned investigators have not had the opportunity to do so. This institutional knowledge enables CARD team members to bring valuable insight and expertise to these time-sensitive investigations. When the life of a child is in possible danger, people want highly qualified investigators as every minute counts when a child is reported missing.

Case Examples

- In 2011, CARD assisted in a child abduction investigation in Colorado City, Texas, by providing several investigative strategies, including the establishment of the Missing/Abducted Child Excel (MACE) application. MACE helped track the completion of the neighborhood canvass; identify suspects; run multiple timelines on the victim, witnesses, and suspects to identify discrepancies and any window of opportunity; and monitor evidence collected during the investigation.[1]
- In 2010, the CARD team responded to a child abduction investigation in Greeley, Colorado. CARD employed strategies throughout the investigation, including a neighborhood canvass, interviews of registered sex offenders, and victimology.
- In 2009, the CARD team provided assistance in a child abduction case in South Carolina. CARD helped to structure the command post, refine lead tracking, coordinate with the Behavioral Analysis Unit 3 (BAU-3) regarding possible abductors, formulate a strategy to locate the abductor, and guide the search and recovery teams. As a result, the child was recovered.
- During an abduction in Nashville, Tennessee, in 2009, the CARD team and BAU-3 advised the execution of basic missing child techniques, such as conducting a neighborhood canvass, reviewing surveillance videos, and focusing media strategies. As a result, the suspect and victim were located. The victim was recovered alive, and the suspect was arrested.[2]
- A child abduction case in Dickinson, Texas, involved an 8-year-old victim who was brutally abducted and raped, had her throat slit by the subject, and was left for dead. In 2008, 18 years later, an FBI agent presented this case at a CARD conference where team members recommended that agents use new technologies and reanalyze the DNA evidence. As a result, agents identified and arrested the subject.[3]
- During a 2007 child abduction case in North Carolina, the CARD team advised the case agent that the victim likely was deceased and hidden somewhere in the individual's residence. The following day, the victim—dead for several weeks—was found in the attic.

Additional Resources

The Cellular Analysis Survey Team (CAST) members also deploy with CARD team members to provide their expertise by exploiting telephone data and performing cellular tracking. They have proven invaluable to child abduction investigations.

In addition, representatives from BAU-3 deploy with CARD. These investigators specialize in victimology, offender typology, and criminal psychology. ✦

Endnotes

[1] Special Agent Michael Conrad, e-mail correspondence to author, September 20, 2010.

[2] Based on FBI investigation.

[3] Special Agent Leonard Johns, e-mail correspondence, April 27, 2011.

Ms. Douglas, an intelligence analyst with the FBI's Criminal Investigative Division, prepared this Crimes Against Children Spotlight.

© Thinkstock.com

Incorporating Hot-Spots Policing into Your Daily Patrol Plan

By Gary Hoelzer and Jim Gorman

Imagine several majors and captains pooling their resources to begin a commercial fishing venture. They buy a fleet of boats, hire well-trained casters, and purchase a beautiful 600-acre lake. Then, they strategize how to catch the most fish and make their business profitable. Experienced fishermen know that the fish do not distribute themselves evenly throughout the water, and, thus, the crew does not disperse the boats evenly throughout the lake. They will use technology or, simply, knowledge of the lake to determine where to drop their lines and nets. Dispersing the boats randomly would be ludicrous and would invite financial disaster on the commercial venture.

Ironically, the strategies that fishermen know would fail in the fishing business mirror those employed by some administrators who deploy patrol officers. They expect their officers to catch criminals with only occasional results. If fishermen fished like such officers patrol, they would catch no haul; but, if officers patrolled like fishermen fish, criminals would go to jail, and crime would decrease. You simply fish where the fish live, and you patrol where crimes occur.

BACKGROUND

"You're poaching!" I first heard those words in 1981 during my field training at the St. Louis,

Missouri, Police Department from other officers who accused me and my field training officer of initiating car stops, pedestrian checks, and arrests in their jurisdictions. My field training officer and I were guilty as charged, for we routinely ventured several miles away from our assigned location (a mostly residential area) to patrol a major retail and entertainment strip. As we began the midnight watch, the residents in our jurisdiction turned out the lights; but, in the neighborhoods to our north, the action was just getting started. My training officer realized that other areas needed our additional presence. Other officers remained territorial about their assignments, but the supervisors appreciated our additional presence in that lively section of the precinct.

> **"By targeting specific crimes in the hot spots, violent crime dropped dramatically while community perception of the police and of the safety of their neighborhoods increased."**

Like my training officer, in the mid- to late-1980s, criminologists noticed that crime and disorder generally occur in clusters, rather than an evenly spread-out manner, throughout geographical jurisdictions. Experts, with the assistance of Minneapolis police and city officials, conducted an influential study on the clusters of crime and disorder. In that city, only 3 percent of the addresses produced 50 percent of the reported crime.[1] When the police department merely transferred officers out of low-crime areas and into those identified as "hot spots," both crime and disorder decreased. These eye-opening results spawned additional federally funded studies.

Spurred by the success in Minneapolis, the National Institute of Justice conducted the Kansas City Gun Experiment and the Indianapolis Directed Patrol Project. These experiments took the Minneapolis approach even further by instructing officers to employ specific strategies as they patrolled the hot spots, or "dots." By targeting specific crimes in the hot spots, violent crime dropped dramatically while community perception of the police and of the safety of their neighborhoods increased.[2]

By the 21st century, it became clear that incident-based officer deployment more effectively reduces crime and disorder than distributing officers in general geographic areas. A National Academy of Sciences panel concluded:

> "(S)tudies that focused police resources on crime hot spots provide the strongest collective evidence of police effectiveness that is now available. On the basis of a series of randomized experimental studies, we conclude that the practice described as hot-spots policing is effective in reducing crime and disorder and can achieve these reductions without significant displacement of crime control benefits. Indeed, the research evidence suggests that the diffusion of crime control benefits to areas surrounding treated hot spots is stronger than any displacement outcome."[3]

FROM GEOGRAPHIC BOUNDARIES TO COPS ON THE DOTS

When large departments with sufficient support personnel identify a hot spot, they typically assign special squads of officers to cover them. An agency might call such a squad a community action team (CAT), neighborhood enforcement team (NET), mobile reserve, or tactical operations. As large departments can handle high demand for service, these teams are deployed to a location for a specified period of time and then move to another

hot spot. While such teams are effective when they cover a particular area, they seldom remain a permanent fixture in any location; thus, the ultimate responsibility for a hot spot, even in a large agency, falls to the patrol officer assigned to that area.

The vast majority of law enforcement agencies in the United States employ less than 50 officers and do not have the resources to form action teams to address hot spots. They assign officers to geographical locations to conduct field investigations, traffic enforcement, calls for service, and other services expected of uniformed patrol. For a typical agency to address hot spots, it needs to develop deployment plans that minimize geographical boundaries, maximize incident-based deployment, and maintain general patrol services. In other words, put the "cops on the dots."[4]

To implement hot-spots policing, agencies first must analyze where crime and disorder clusters in their jurisdictions. Small jurisdictions can chart this effectively with a pin map, but larger agencies need computerized crime mapping. When departments identify a specific problem in a particular geographical area, they highlight it as a "common patrol area," or CPA. To execute CPA deployment, agencies should—

- determine geographical hot spots for crime and disorder;
- designate the sectors responsible for patrol;
- develop strategies at the operational level to address the crime or disorder problem;
- analyze the issue for community input and involvement;
- determine if the CPA will be a permanent designation due to an at-risk location (e.g., retail centers) or temporary due to an ongoing crime spree;

Figure 1. Common patrol areas circled

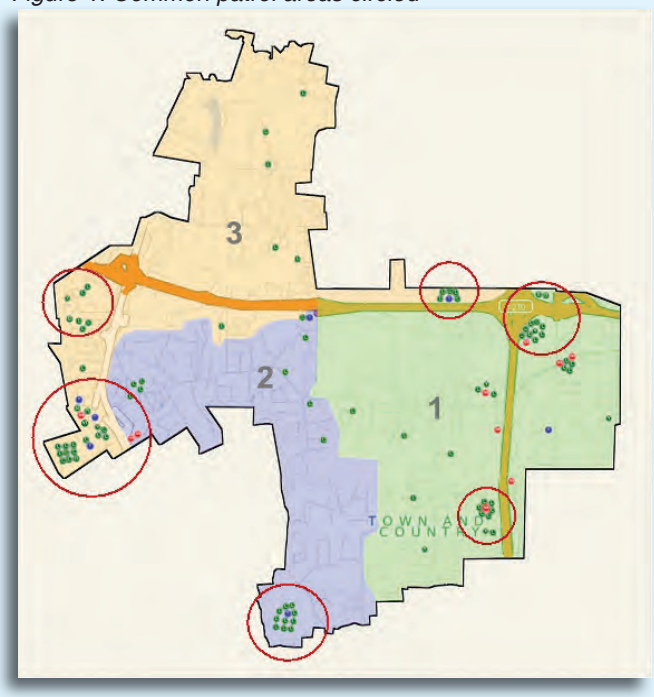
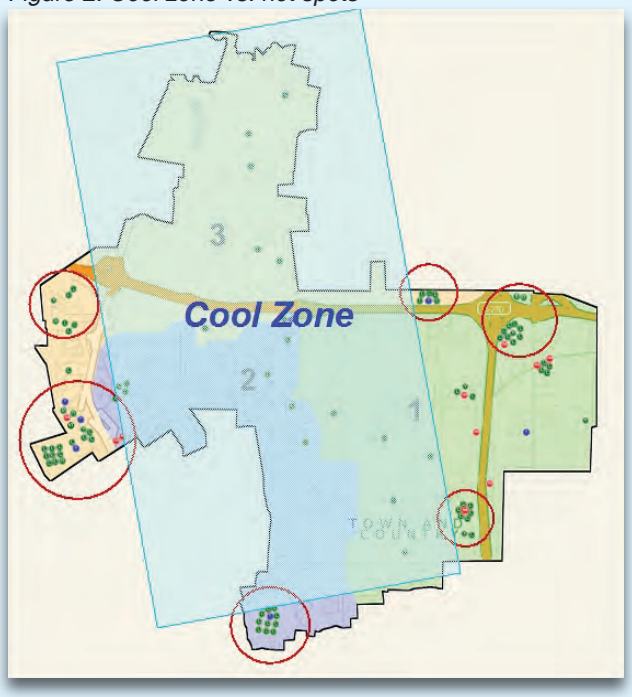


Figure 2. Cool zone vs. hot spots



- direct routine patrols to the CPA without requiring permission to cross geographical sector boundaries; and
- track the numbers of patrols and outcomes.

Once a department identifies a CPA, the adjoining sectors share responsibility for the area, which adds supervisor patrols and support units. This system more than triples the number of patrols in CPAs, but maintains reasonably quick response times in low-incidence locations.

OUR EXPERIENCE

Located in the heart of the St. Louis metropolitan area, the Town and Country Police Department (TCPD) transitioned from traditional geography-based to incident-based patrol deployment using CPAs. The department still assigns patrol officers to geographical sectors, but CPAs make an officer's boundaries more fluid. With incident-based deployment, TCPD integrates the intuition and knowledge of experienced patrol officers, like my field training officer, into formal organizational plans.

Early in 2010, TCPD further reduced the emphasis on geographical assignments with the Positioning Units Strategically in Hot Spots (PUSH) program. The program was developed to build on the CPA concept in one particular location, an 11-square-mile city in the St. Louis suburbs. Three sectors (with one officer to patrol each) comprised the jurisdiction, but it was mostly a "cool zone" that experienced little criminal activity.

With PUSH, we consolidated the three sectors into an east patrol and a west patrol and then assigned one officer to each. This leaves the third officer unassigned to any one geographical area so that supervisors can "PUSH" this officer to a location when a problem emerges.

The PUSH plan focuses on clusters of incidents (the dots) as the primary basis for deployment, rather than geographic boundaries. Our latest crime maps illustrate that most dots appear in the southwest or northeast portions of the east patrol; thus, PUSH officers concentrate in those areas.

Figure 3. P.U.S.H. deployment plan

The PUSH program functions like a fictitious war room in World War II movies. In these scenes, military personnel huddle around a large table with long poles in their hands, constantly pushing small shapes around on a map to symbolize moving manpower and resources. As commanders receive intelligence from the field, they move assets accordingly. This fluid approach capitalizes on all available manpower to saturate a hot spot.

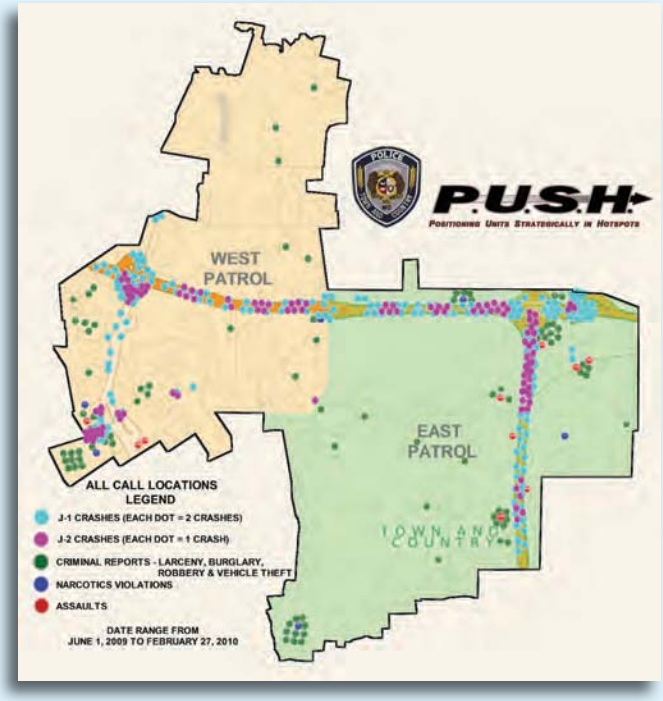
Tactics and Strategies

Targeting the most frequent crimes in a hot spot proves much more effective than merely sending more officers to a problem area.[5] To

supplement the increased patrols, supervisors must develop specific strategies for the CPAs based on the area's most frequent crimes. We analyze crime data by location and time of day, and as soon as we observe a pattern, we tailor our approach to that CPA. This system allocates resources more effectively as we equip officers with the appropriate technology and training to address the specific incidents that occur in those areas.

For example, at TCPD, we designate all malls and shopping centers as CPAs due to the increase in organized retail theft; therefore, officers target this crime when they patrol these areas. Officers partner with store security, issue "no trespass" warnings to identified thieves, install license-plate-recognition technology, conduct foot patrols, and target repeat offenders; they also have developed a business watch network. These tactics specifically target organized retail theft and, thus, reduce crime in malls and shopping centers.

Figure 4. Crime and traffic crash activity



Similarly, in 2009, our department noticed increasing reports of "car hopping," or walk-by thefts of items from parked vehicles. We tailored our patrol in those areas where our crime analysis revealed that car hopping occurred frequently. In one such area, an arterial roadway running through the center of Town and Country, residents reported thefts from vehicles, garages, and homes in the overnight hours. Shortly after we identified the common patrol area, a sergeant patrolling along the roadway around 3:00 a.m. observed a vehicle that resembled one of those sighted in previous thefts. The officer stopped the car in a residential area and identified three occupants who had, in fact, been arrested approximately 1 year earlier for other burglaries and thefts from vehicles. After he apprehended the driver for driving with a suspended license, the officer communicated the intelligence to our detectives. They, in turn, investigated the suspects' involvement in the related crimes.

Even further, CPA and crime-targeted patrols grant officers the opportunity to use their own ideas, expertise, and experience to develop strategies for different areas. The approaches that officers can apply to a CPA are as extensive as their imaginations, including all of the tools that community policing and problem solving bring to the "war-room table."

Data-Driven Approaches to Crime and Traffic Safety

Incident-based deployment relates not only to criminal activity but also to important public safety issues, such as traffic crashes. When we include traffic incidents on the crime map of Town and Country, the number of dots explodes [see Figure 4]. Six miles of interstate highway run through the city, and this hot spot of crash activity

costs millions of dollars and several hundred injuries annually. When we discovered these results, we realized the need for a unit for interstate traffic enforcement and crash reduction. Simply by including crash data in our incident-based deployment analysis, we identified a dangerous public safety issue and took steps to remedy the problem.

The National Highway Traffic Safety Administration studies these issues all around the country through the Data-Driven Approaches to Crime and Traffic Safety (DDACTS) program. Because crimes often involve motor vehicles, and highly visible traffic enforcement deters crime, the program integrates location-based crime and traffic crash data. DDACTS then studies this data and employs geomapping to identify areas with high rates of crime and crashes. This approach closely mirrors incident-based deployment, and it provides an effective strategy to both fight crime and reduce traffic accidents and violations.[6]

> **"This system allocates resources more effectively…to address the specific incidents that occur in those areas."**

CONCLUSION

These economic times challenge law enforcement agencies to accomplish more with fewer resources. To respond to this conundrum, at the Town and Country Police Department, we embrace the philosophy of incident-based deployment, or hot-spots policing. We reduced the number of officers unoccupied during their patrol by deemphasizing geographical assignments or consolidating them and using the extra officers to patrol hot spots, allowing us to maximize limited resources and control crime. These deployment plans also wed policy with practice by capitalizing on the latest academic research on situational crime prevention. Hot-spots policing, like our PUSH program, efficiently allocates an agency's resources to those that need them most, whether the agency employs 5 officers or 5,000.✦

Endnotes

[1] David Weisburd and Anthony Braga, eds., *Police Innovation: Contrasting Perspectives* (Cambridge: University Press, 2006).

[2] Dennis P. Rogan, James W. Shaw, and Lawrence W. Sherman, "The Kansas City Gun Experiment," *National Institute of Justice: Research in Brief* (Washington, DC, January 1995).

[3] Wesley Skogan and Kathleen Frydl, ed., *Fairness and Effectiveness in Policing: The Evidence* (Washington, DC: National Academies Press, 2004), 250.

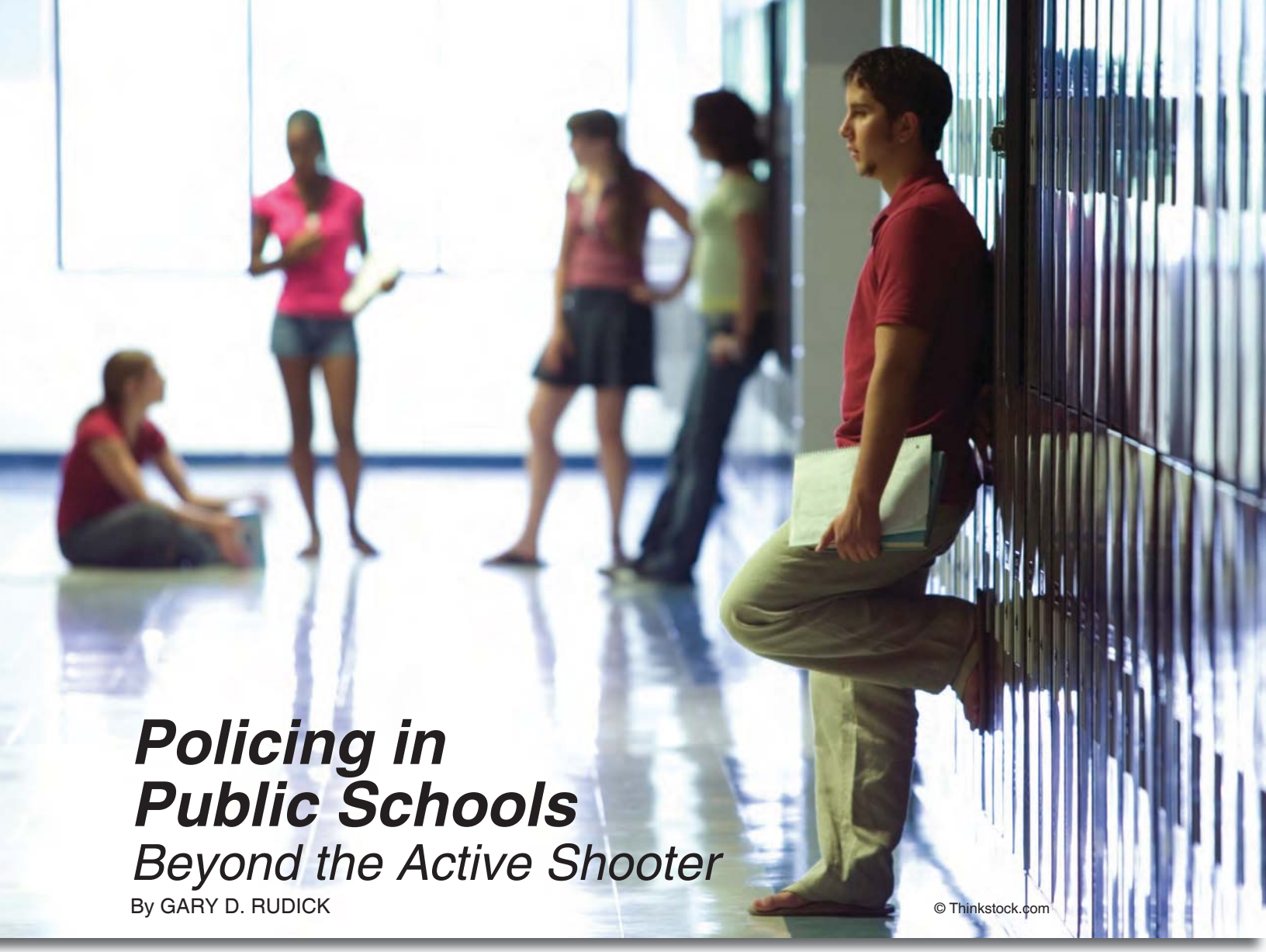
[4] Jack Maple and Chris Mitchell, *The Crime Fighter: How You Can Make Your Community Crime Free* (New York, NY: Doubleday, 1999).

[5] Steven Chermak, Edmund McGarrell, and Alexander Weiss, U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, *Reducing Gun Violence: Evaluation of the Indianapolis Police Department's Directed Patrol Project*, NCJ 188740 (Washington, DC, 2002).

[6] U.S. Department of Transportation, National Highway Traffic Safety Administration, and U.S. Department of Justice, Bureau of Justice Assistance, National Institute of Justice, "Data-Driven Approaches to Crime *and* Traffic Safety (DDACTS)," *http://www.nhtsa.gov/DOT/NHTSA/Traffic%20Injury%20Control/Articles/Associated%20Files/811186.pdf* (accessed September 12, 2011).

Captain Hoelzer serves with the Town and Country, Missouri, Police Department.

Officer Gorman serves with the Town and Country, Missouri, Police Department.



Policing in Public Schools

Beyond the Active Shooter

By GARY D. RUDICK

© Thinkstock.com

Violence that occurs in public schools is not new. Nothing chills the heart and soul of parents and other members of the public as much as an unprovoked, violent attack against school children. Unfortunately, the number of these crimes has grown in schools across the nation because public education mirrors society as a whole. The students of today differ from those of a half century ago, and schools paired with violent neighborhoods and unsafe communities present even greater danger.

To keep schools safe, educators have instituted more aggressive security measures and demanded a greater presence of municipal and county law enforcement on campuses. As a result, state and local governments have passed legislation to create new campus law enforcement agencies. As the nation's fear of violence in public schools increases, the pressure placed on police agencies to protect the educational environment increases as well.

Indeed, an armed intruder presents the gravest threat to the school population, and campus police officers train rigorously for active-shooter scenarios. Unfortunately, safety threats are not confined to violent intruders on campus. In fact, the active-shooter threat occurs even more

rarely when compared with the consistent risks to students, faculty, and staff. Crimes, like physical assault, possession of weapons or drugs, and theft, occur much more frequently than armed intrusions, yet the public and most of law enforcement remain largely unaware of these incidents. Additionally, officers may have to deal with difficult situations that involve students with special needs, youngsters living in poverty, irate parents, disgruntled faculty, and principals dealing with the pressure to meet certain levels of achievement, at times at the expense of their school's safety.

The situations described above pertain exclusively to educational environments, and most law enforcement officers are not trained to handle them. Therefore, campus police officers must receive targeted training to learn how to respond to all of these scenarios. A training curriculum confined to the armed intruder threat will prove insufficient for a campus police department. To increase law enforcement's effectiveness in schools, agencies must prepare officers for all aspects of public school policing.

Law enforcement administrators should ask themselves, What sort of instruction in addition to active shooter training will benefit police personnel in public schools? Are certain policing techniques truly unique to an educational setting? Will street officers' training prepare them to serve in an educational setting and protect the school in different scenarios? As a chief of police for a public school police agency, the author offers suggestions based on his own experiences to tailor training for law enforcement within an educational setting.

STUDENTS WITH SPECIAL NEEDS

Individuals with Disabilities Education Act

A 17-year-old male student who has the mental capacity of a 6 year old rapes another mentally challenged male student who is deaf and mute. The school administrators attempt to interview the suspect and witnesses to determine if a crime has been committed. Because of the serious handicaps of the students involved, administrators consider the situation an internal matter and do not contact law enforcement to conduct a criminal investigation. The suspect's parents remove him from the school and place him in a mental institution. By the time administrators call the police a day later, forensic evidence has been compromised, and potential witnesses are considered unreliable. The investigation has been weakened so badly that the officers cannot file criminal charges.

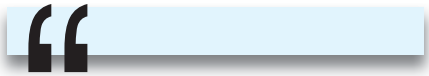
Many school administrators hesitate to report crimes committed by students with disabilities. They assume that

> ***"As the nation's fear of violence in public schools increases, the pressure placed on police agencies to protect the educational environment increases as well."***

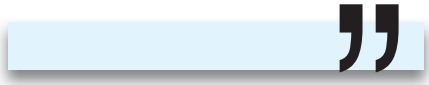
Chief Rudick serves with the Tulsa, Oklahoma, Public Schools Campus Police.

an incident involving a student in a special education program requires a different course of action than one involving the average student. Indubitably, crimes that manifest from a diagnosed disability present significant complications for investigators. To learn more about these situations, police officers who work within schools should familiarize themselves with the Individuals with Disabilities Education Act (IDEA). The federal law states that, "Educators are not exempt from reporting criminal conduct by a child with a disability to the appropriate authorities. Nothing in this subchapter shall be construed to prohibit an agency from reporting a crime committed by a child with a disability to appropriate authorities or to prevent state law enforcement and judicial authorities from exercising their responsibilities with regard to the application of federal and state law to crimes committed by a child with a disability."[1]

Many school and law enforcement officials misinterpret the regulations presented in IDEA. In some cases, school officials have prevented police officers from handcuffing special education students under arrest. In other instances, school employees have abandoned their own responsibilities to restrain students, or police officers have used an inappropriate type or level of force. How will officers know how to act in these situations when even education professionals do not always know the proper protocol? Instructing officers about how IDEA applies to their work will help them respond to these sensitive situations safely, appropriately, and legally.



Officers…in schools should be well versed in the nuances and regulations of IDEA as courts may apply criminal statutes differently to cases involving special education students.



Language of Special Education

A student becomes unruly in class to the point that the teacher fears the boy will harm someone. The teacher physically forces the child to sit down, and a struggle ensues. The student's Individual Education Plan (IEP) states clearly that a teacher can touch the child using only a certain technique that requires specific training. When the child's mother learns of the incident, she demands a formal police report, claiming the teacher's physical contact violated the IEP. She wants to file criminal assault and battery charges against the teacher.

Law enforcement administrators should ask their officers certain questions to ensure they understand the regulations they must follow. These questions should include, Do you know what an IEP is? Can you explain why officers need training regarding special restraint techniques? Can school officers view confidential documents about special education students? Do federal requirements for reporting mechanical restraints include handcuffs? These topics all relate to campus law enforcement, yet most campus police agencies do not include them in training.

Today, federal laws have begun to require that every school employee, including security personnel and campus police, receive training to learn how to appropriately restrain special education students when necessary. If personnel fail to complete or document this specialized training, it can result in serious civil penalties for schools and individual employees. Officers working in schools should be well versed in the nuances and regulations of IDEA as courts may apply criminal statutes differently to cases involving special education students.

Additionally, officers benefit from learning about the students with special needs in their school so that they know how to interact and communicate with each of them. An IEP can help officers gather this critical information. This document details the preferred methods of instruction and discipline for a special needs child. This can be as simple as "John needs additional time to complete exams" or as serious as "Susan requires a personal aid throughout the day." This information helps officers and faculty avoid using unnecessary force against these students and encourages alternative methods to calm them during violent episodes.

Traditional tactics of forceful restraint, including handcuffing techniques and physical restraints, may not prove effective when dealing with special needs students. School police officers should receive training to learn about topics, such as legal access to student records, release-of-information laws, and the acceptable methods of physically handling students.

EFFECTS OF GENERATIONAL POVERTY

A middle school student disrupts a class, curses at his teacher, and, later, starts a fight with another student. When he arrives at police headquarters, he is angry and confrontational. After a period of time, he calms down and confesses that last night, his older brother was shot while standing in the front door of their home. The student jumped out of his bedroom window and ran away from the house to escape the gunfire, but he had no place to go for protection. He admits that this event caused him to feel angry all day at school. He then asks for something to eat as he has not eaten anything since lunch the previous day.

As human beings, officers bring their own personal experiences and values to the job and, thus, may have preconceived notions concerning academic performance and behavior in the educational environment. However, students raised in different socioeconomic circumstances, especially in generational poverty, might maintain a different perspective. Common views on education, money, and, even, humor may differ between the economic classes and cause misunderstandings.

Becoming more cognizant of how a student's socioeconomic background impacts their behavior may help officers increase understanding, improve communication, and reduce conflict. As one excellent resource, school police officers can reference the book *A Framework for Understanding Poverty* for insights on this topic. Police officers could benefit from applying the principles of this book to their own relationships with people in poverty, particularly students.[2]

PRINCIPAL'S PERSPECTIVE

A school police officer once reported, "I don't understand. The kids are walking the halls, won't go to class, and won't obey any instructions. They let the kids get away with all sorts of bad behavior and then wonder why things get out of hand and fights start. What is wrong with this principal that he won't make an example of these kids? If they are not here to learn, kick them all out of school!"

Police officers do not experience the same pressures placed on school administrators who need to achieve adequate annual yearly progress or meet the federal mandates of No

Child Left Behind. The law requires that schools lead students to earn certain scores in math, reading, science, social studies, and attendance each year. Failing to reach these standards can cost a school its funding and principals or superintendents their jobs. Principals must achieve success in these critical areas while dealing with other stressors, such as special education, student testing, athletic excellence, and union contract negotiations.[3]

The above scenario described an officer's actual experience in a school that failed to improve test scores enough to satisfy federal and state requirements, largely because too few students attended the tests. As a result, school administrators ignored unacceptable behavior just to keep enough students in the building. If the school suspended students for behavior violations, too few would be able to take the exams, and the school would not achieve the necessary improvements. While the officer felt frustrated at how this policy negatively impacted the school's safety, it, nonetheless, helped the school reach its mandated progress and come off of the "needs improvement" list.

Officers could benefit from training sessions that focus on the administrative expectations placed on principals. Such knowledge would reduce misunderstandings between campus police and education officials. Also, this training may facilitate ideas for handling students in ways that satisfy both the officer's desire to keep the school safe and the principal's need to achieve certain education goals.

> ***"To understand how to police this unique environment, law enforcement personnel need to receive training to sensitize them to the needs of the students, faculty, and staff."***

TEACHER FACTOR

A police officer receives a call to arrest a student for assault and battery. The involved teacher physically had blocked the door to prevent the student from leaving the classroom, but the boy shoved past her. The officer determines the student had no criminal intent to harm and only exited the room out of frustration and to prevent conflicts with other students from escalating. With no intent, the officer determines the boy committed no crime and makes no arrest. The teacher files a formal complaint that alleges the officer refused to perform his duty. She tells others that the police do not care about the safety of the faculty.

To prevent such misunderstandings, training sessions should create shared opportunities for officers and educators to learn about certain topics together. This facilitates mutual understanding of each profession's respective duties within the school environment.

In 2009 and 2010, the Oklahoma Council on Law Enforcement Education and Training sponsored events in Tulsa and Oklahoma City that embraced this unique training philosophy. The topics were presented in 1-hour blocks during which educators (superintendents, principals, counselors, and teachers) and police officers (from municipal, county, state, and campus police departments at both the college and secondary levels) came together for professional instruction on important issues. Topics included criminal laws specific to schools and juvenile violators, media relations, creation of safe school environments, special education students, and public release of information involving students. The attendees could ask questions and receive feedback

from both law enforcement and education perspectives. Both groups came away with a better understanding of each other's duties, responsibilities, misconceptions, and concerns.

CONCLUSION

Policing in an educational setting truly is a unique responsibility. It presents special challenges because the school environment differs so greatly from the jurisdictions of most other law enforcement agencies. To understand how to police this unique environment, law enforcement personnel need to receive training to sensitize them to the needs of the students, faculty, and staff.

Former First Lady Laura Bush said, "Children can't learn if they're worried about their safety."[4] Obviously, school police officers must be prepared to protect their school from violent crimes and armed intruders. But, their training must expand beyond the active-shooter scenario. If campus police departments intend to make schools a safer and more secure environment for learning, they must prepare their officers. This will demonstrate law enforcement's commitment to serve the most vulnerable of citizens—children.✦

Endnotes

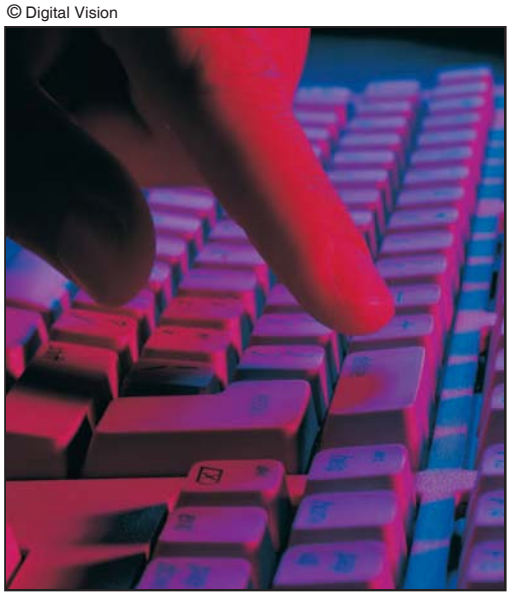
[1] U.S. Department of Education, "Individuals with Disabilities in Education Act," *http://www2.ed.gov/Policy/speced/guid.html* (accessed January 9, 2011).

[2] Ruby K. Payne, *A Framework for Understanding Poverty* (Highlands, TX: aha! Process, Inc., 1998).

[3] U.S. Department of Education, "No Child Left Behind," *http://www2.ed.gov/nclb/landing.jhtml* (accessed January 9, 2011).

[4] Gannett News Service Multimedia, "Safe at School? A National Forum for Ideas and Discussion," *http://azcentral.gns.gannettonline.com* accessed January 21, 2011).

The *Bulletin's* E-mail Address



The *FBI Law Enforcement Bulletin* staff invites you to communicate with us via e-mail. Our e-mail address is *leb@fbiacademy.edu*.

We would like to know your thoughts on contemporary law enforcement issues. We welcome your comments, questions, and suggestions about the magazine. Please include your name, title, and agency on all e-mail messages.

Also, the *Bulletin* is available for viewing or downloading on a number of computer services, as well as the FBI's home page. The home page address is *http://www.fbi.gov.*

Leadership Spotlight

Learning from Failure

"Success is a lousy teacher. It seduces smart people into thinking they can't lose."
— Bill Gates, Founder and Chairman of Microsoft

Failure is part of the learning process. It occurs everywhere and at any time. It shapes our experiences: who we are, how we lead, and what our organizations ultimately become. Failure can occur in our professional and personal lives, but it is how we deal with and transcend it that really counts. For most of us, dealing with failure is an uncomfortable and unnatural behavior. Typically, many of us would like to run away when it occurs and for things to return to the status quo as soon as possible. But, allowing our leaders, managers, and employees to quickly forgive and forget may lead to major consequences in the future. If we do not work to improve upon failure, it inevitably will occur a second time.

Examining what went wrong is critical to the future success of those affected by failure. For that reason, the U.S. military conducts after-action reports and debriefings, and the FBI National Academy conducts "hot washes" after each 10-week session. Jack Welch, former chairman of General Electric, called it "examining the car crashes," and Jim Collins, a notable leadership guru and author, referred to it as "conducting autopsies."

I propose using a RADICAL (review, analyze, diagnose, independent, candid, accountable, and learn) departure from how you traditionally have viewed and acted toward failure. The purpose is to conduct an in-depth review of the failed project or event. First, bring all parties back together at an appropriate time; the closer to the end of major operations the better. Analyze all facets of the recent failure, to include logistics, administration, decision making, timing, job responsibilities, coordination, and leadership. Diagnose the true reasons of failure without any talk of remedies or solutions. Independently verify why the failure occurred through objective or external means. In this step, be candid and do not hold back; honesty and frankness must be part of examining failure. Accountability regarding specific roles and responsibilities needs to be ferreted out. Most likely, the finger pointing began soon after the failure occurred.

Finally, learn from the failure. Determine what occurred, why it happened that way, and what can be done better next time. Will additional training and education help? How can you avoid the same pitfalls and traps next time? Will your systems and processes become more efficient? This final step serves to address these questions and allows you to come away smarter, better, and more productive the next time around.

Do not let these learning moments slip away, especially when our natural tendency is to run from failure. As noted statistician Dr. W. Edwards Deming once said, "Managers who focus on failure become experts on failure." ✦

Special Agent Gregory M. Milonovich, an instructor in Faculty Affairs and Development at the FBI Academy, prepared this Leadership Spotlight.

Supreme Court Cases
2010-2011 Term

By MICHAEL J. BULZOMI, J.D.

Each year, the U.S. Supreme Court decides cases that impact the everyday operations and management of law enforcement agencies. The 2010 to 2011 term was no different. It included case decisions covering a variety of constitutional and statutory issues that will affect how departments conduct business.

In this term, the Court decided two Sixth Amendment Confrontation Clause cases and one municipal liability case of interest. It also addressed the protection afforded speech in a case involving a government employee. In the criminal genre, there was a case centering on the emergency exception to the Fourth Amendment search warrant requirement, along with a juvenile case addressing the relevance of age and Miranda warnings. The Court also addressed the scope of retaliation protection under the Fair Labor Standards Act (FLSA) and in a traditional claim of discrimination in a Title VII case. The Court also decided a bias case involving the Uniformed Services Employment and Reemployment Rights Act (USERRA). The final case involved alleged government retaliation for an employee's exercise of the First Amendment right to

petition grievances against the government.

This article provides brief synopses of these cases. As always, law enforcement agencies must ensure that their own state laws and constitutions have not provided greater protections than those offered by U.S. constitutional standards.

Michigan v. Bryant, 131 S. Ct. 1143 (2011)

In this case, the U.S. Supreme Court decided that statements made during an ongoing emergency by an unavailable witness are not barred from admission at trial and that their admission does not violate the Sixth Amendment Confrontation Clause. On April 29, 2001, at approximately 3:30 a.m., Detroit police officers responding to a radio dispatch found a man critically wounded in the parking lot of a gas station. The man, Anthony Covington, was questioned as to what happened, who shot him, and where the shooting had occurred. He responded that he had been shot by respondent Bryant at Bryant's house and that he had driven himself to the gas station. Covington died hours later. His statements were used by the police in Bryant's murder trial where Bryant was convicted of second degree murder. Bryant's conviction was reversed by the Michigan Supreme Court, which held that the Sixth Amendment Confrontation Clause rendered Covington's statement's inadmissible testimonial hearsay.[1]

Special Agent Bulzomi is a legal instructor at the FBI Academy.

The case was appealed to the U.S. Supreme Court, which held that testimony by police officers at a murder trial regarding the dying victim's identification of the defendant did not violate the defendant's rights under the Confrontation Clause. Because the primary purpose of the victim's statements was to enable police to respond to an ongoing emergency—a shooting—they were admissible at Bryant's trial.[2]

The Court provided two rules to guide the inquiry as to whether the Confrontation Clause would bar a statement. First, the primary purpose test considers the perspectives of both interrogators and the interrogated. In other words, a witness can answer even questions asked in good faith in a way that makes their primary purpose testimonial. Second, the test is objective; to determine primary purpose, courts should look at the purpose that reasonable people would have in eliciting or giving the statement, rather than at the actual motives of the parties. If the statement was made to meet an ongoing emergency, its primary purpose usually will be innocent. Whether the emergency is ongoing even after the crime is completed turns largely on the extent of the continuing public danger—an assessment that could depend on the weapon used in the crime, the likelihood that the assailant will strike again, the medical condition of the victim, and other case-specific circumstances.[3] The Supreme Court determined that the statements at issue were obtained primarily for investigative purposes, and, thus, their use at trial did not violate the Sixth Amendment.

Bullcoming v. New Mexico, 131 S. Ct. 2705 (2011)

The Court decided that the testimony of a lab analyst who had no role in the testing of trial evidence would not satisfy the Sixth Amendment Confrontation Clause requirements. The

petitioner, Donald Bullcoming, was arrested for drunk driving. Tests revealed that his blood-alcohol level was three times the legal limit. Prior to Bullcoming's trial, the lab analyst who had conducted the tests and signed the lab reports had been placed on unpaid leave, so another lab analyst was called to the stand to testify concerning the report. The analyst who testified had neither participated in nor observed the performed tests. The Supreme Court of New Mexico decided that it was not necessary for the lab analyst who conducted the tests to testify as long as a lab analyst testified that the Sixth Amendment Confrontation Clause would be satisfied.[4]

The U.S. Supreme Court disagreed. In 2009, it had decided in *Melendez-Diaz v. Massachusetts* that a lab report was a form of testimony; as such, the Confrontation Clause required the authors of the report to take the stand for cross-examination.[5] Here, the question was whether another lab analyst could testify in place of the one who actually performed the tests. In a 5 to 4 decision, the Court determined that testimony by a substitute witness does not satisfy the Confrontation Clause. The Court reasoned that given the nature of the examination, a defendant must have an opportunity to dissect the examiner's work by way of confrontation.[6]

Connick v. Thompson, 131 S. Ct. 1350 (2011)

In this case, the Court decided that the district attorney's office should not be held liable under Section 1983 for failure to train its prosecutors based on a single *Brady* violation.[7] Thompson was convicted of murder, sentenced to death, and served 17 years in prison, where he came within a month of his execution date. He had chosen not to testify at his trial because of his fear that the prosecution would bring up an earlier conviction for armed robbery to try to make him look less believable.

However, unbeknownst to Thompson and his attorneys, the prosecutor had blood evidence that would have exonerated him from guilt in the armed robbery case. Had he not been convicted of armed robbery, he could have testified in his own defense in the murder case, and the outcome could have been different. In fact, he was acquitted in a new trial once the blood evidence came to light. After his release from prison, Thompson filed a federal civil rights lawsuit pursuant to Title 42, Section 183, U.S. Code against the district attorney's office, alleging that a *Brady* violation involving the failure to disclose the exonerating blood evidence was caused by the office's deliberate indifference to an obvious need to train its prosecutors to avoid such constitutional errors.

The U.S. Supreme Court found that although the prosecutors should have given Thompson the blood evidence, when misconduct by prosecutors leads to a wrongful conviction, the agency can be held liable for

its employee's actions only if the policy maker for the agency was aware of a pattern of similar bad behavior in the office, yet still did not start a training program for prosecutors. In *City of Canton, Ohio v. Harris*, the Court noted that it had, in fact, left open the possibility that the unconstitutional consequences of a single incidence of failure to train could be so patently obvious that a city could be held liable under Section 1983 without proof of a preexisting pattern of violations.[8] However, the Court noted that this was not such a case as lawyers are equipped with the tools to seek out, interpret, and apply legal principals prior to obtaining their positions with the government, so additional training would not necessarily be required for them to do their jobs within the confines of the Constitution.[9] Thus, a single *Brady* violation would not constitute deliberate indifference; a pattern of similar violations would be necessary to establish that a "policy of inaction" constituted the functional equivalent of a decision by the city itself to violate the Constitution.

Snyder v. Phelps, 131 S. Ct. 1207 (2011)

According to the U.S. Supreme Court, political picketing at a military funeral, even if offensive in its content and manner, is constitutionally protected

if it addresses matters of public concern. Fred Phelps, the founder of the Westboro Baptist Church in Topeka, Kansas, and six of his followers picketed the funeral of Marine Lance Corporal Mathew Snyder, an Iraq War veteran. The protest centered on their belief that God hates the United States for its tolerance of homosexuality. The protestors verbally conveyed their message of intolerance and used signs with messages, such as "Thank God for Dead Soldiers" and "America is Doomed." The protest was regarded as peaceful and occurred on public property approximately 1000 feet from the church holding the service.

Snyder's father sued Phelps and his church under state tort law, alleging intentional infliction of emotional distress and invasion of privacy. A jury found Phelps and his church liable for millions of dollars in compensatory and punitive damages.

Phelps appealed, arguing that the First Amendment is violated when a state law allows for infringement on First Amendment protected speech. The Fourth Circuit Court of Appeals reversed the jury determination, granting First Amendment protection for the speech because it centered on matters of public concern, was not provably false, and consisted of participants expressing it solely through hyperbolic rhetoric.[10]

The case also was appealed to the U.S. Supreme Court, which recognized that the contours of what constitutes protected speech is not well defined. However, speech still is protected despite its repugnant nature when it addresses a matter of public concern. The Court has determined that speech relating to matters of political, social, or general interest, value, or concern to the community generally is a matter of public concern. The Court advised that an examination of a statement's content, form, and context decides a matter of public concern, not its inappropriate or controversial character.

The Court decided that the content of the speech in this case related to public matters, such as the moral conduct of the United States and its citizens, not private concerns. The

context was on social issues and did not involve personal attacks upon Snyder. The speech occurred on public property in a peaceful manner and did not disrupt the funeral. The Court stated that even hurtful speech on public matters is protected to ensure that public debate is not stifled.[11]

Kentucky v. King,
131 S. Ct. 1849 (2011)

The Court determined that an exigent circumstance created by the arrival of law enforcement officers at a residence does not negate the emergency warrant exception. A search of an apartment in Lexington, Kentucky, took place after the controlled purchase of crack cocaine outside the complex. The suspect dealer walked into the apartment breezeway and entered a residence. The pursuing police officers did not receive the radio call with the information as to which apartment the suspect entered. The officers stood between two apartments, not knowing which one the suspect had entered, smelled burning marijuana, knocked on the suspect's apartment door, and announced their presence. The residents of the apartment did not respond, but the officers heard noises indicating that the occupants were in the process of destroying the drug evidence. The police officers announced their intentions to enter; made a warrantless, forced entry; and found three individuals smoking marijuana, as well as, in plain view, cocaine. The officers subsequently found crack cocaine, cash, and drug paraphernalia. The original drug suspect later was apprehended in another apartment.

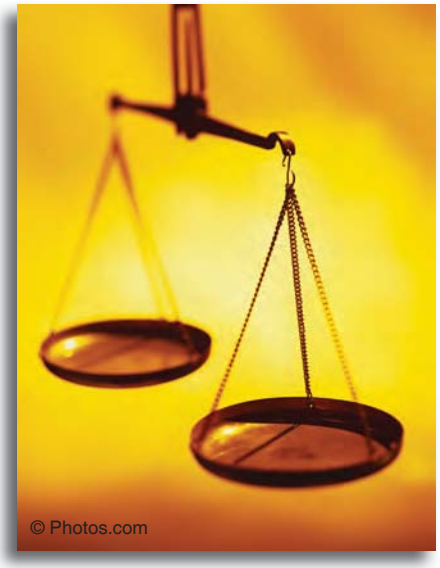
The respondent, Mr. King, one of the three occupants of the first apartment, was convicted of distribution charges and sentenced to 11 years imprisonment. He appealed his conviction. The Kentucky Court of Appeals affirmed his conviction, stating that the entry into the home was justified under the emergency search warrant exception because the police reasonably believed that the drug evidence would be destroyed and that they did not impermissibly create the exigency because they had not deliberately evaded the warrant requirement. The Supreme Court of Kentucky reversed, stating that the police could not rely on the exigent circumstances exception if it was reasonably foreseeable that the investigative technique used would result in the exigent circumstances.[12] Hence, knocking and announcing inevitably would induce the destruction of the evidence.

The U.S. Supreme Court assumed that exigent circumstances existed in this case, meaning there was a reasonable belief that evidence would be destroyed unless entry was made. Because exigent circumstances existed, the only question was whether the actions of the police were allowable. The Court decided that as the officers had not violated or threatened to violate the Fourth Amendment prior to the

exigency, the warrantless entry was justified.[13] The likelihood that the police notifying suspects of their presence will result in the individuals destroying the evidence, thus creating exigency, has no bearing on the validity of a warrantless entry.

J.D.B. v. North Carolina, 131 S. Ct. 2394 (2011)

In this case, the Supreme Court advised that age is a factor when deciding whether to provide the Miranda advice of rights to a juvenile suspect, but clarified that age is not a determining factor. J.D.B., a 13 year old, was pulled out of class and taken to a conference room at his school, where school administrators and a uniformed police officer questioned him about some items stolen from neighborhood homes. J.D.B. eventually confessed to stealing the items.



His attorney later argued that his confession could not be used because he had not received Miranda warnings. The North Carolina Supreme Court rejected that argument.[14] J.D.B. then filed a petition for certiorari in which he argued that because he was a minor, he would not reasonably believe that he was free to leave when confronted by a police officer and, therefore, must receive Miranda warnings prior to being interrogated.

The U.S. Supreme Court reversed the North Carolina Supreme Court. In a 5 to 4 opinion authored by Justice Sotomayor, the Court held that a minor's age can be a relevant factor when determining whether he or she is in custody. The Court reasoned that while the determination of custody is still an objective one, including consideration of a minor's age in that objective determination is appropriate given the psychological differences between adults and juveniles. This is not to say that age is the decisive factor, but it recognizes that age is to be considered given that a reasonable adult may view the circumstances differently than a reasonable juvenile.[15] The case was remanded back to the North Carolina Supreme Court to determine whether the factoring of age into the analysis occurred while J.D.B. was in custody.

Kasten v. Saint Gobain Performance Plastics Corp., 131 S. Ct. 1325 (2011)

The FLSA contains an antiretaliation provision protecting employees who complain of unfair labor practices. However, some question arose as to what kind of complaint qualifies for protection under the act. The FLSA refers to filing a complaint. The act does not specify how this must be done, leaving the Court to determine whether a written complaint is necessary or if an oral complaint satisfies the FLSA. The Court held that a complaint could be filed orally.

Kevin Kasten alleged unlawful retaliation from his employer, Saint Gobain Performance Plastics Corp., which fired him for orally complaining to company officials concerning the location of time clocks, which prevented workers from claiming donning and doffing time for protective gear required for work. The company claimed that it dismissed Kasten after repeated warnings for failing to properly record his comings and goings on the time clock. The district court granted summary judgment in favor of the employer, holding that the act did not allow protection for oral complaints. The Seventh Circuit Court of Appeals affirmed the district court's decision.[16]

The U.S. Supreme Court granted certiorari, holding that

an oral complaint is protected under the FLSA antiretaliation provision. The Court used several different tools of statutory interpretation to reach that result. It pointed out that the dictionary definitions of the word *filed* varied, but that the purpose of the act—to protect employees with legitimate complaints—would be undermined if the act required all complaints to be in writing.[17] The Court also noted that many state legal systems allow for oral filings and that the agency charged with administering the FLSA regarded oral complaints as falling under the act. The Court concluded that the Seventh Circuit Court of Appeals erred in determining that oral complaints do not fall within the scope of the act's antiretaliation provision and left the question of whether Kasten could meet the act's notice requirement for the lower courts to decide. The case was vacated and remanded to the Seventh Circuit Court of Appeals. This ruling lessened the need for a high degree of formality when seeking protection from retaliation based on conduct protected by the FLSA.

***Staub v. Proctor Hospital*, 131 S. Ct. 1186 (2011)**

An employer can be liable for discrimination under the USERRA if a decision detrimental to an employee is influenced by bias, even if the person who actually makes the detrimental decision is not the biased party. Staub was fired after his two immediate supervisors, who were hostile to him in regard to his military reserve status, mandated additional reporting requirements for him, which they later claimed he did not do. This failure to follow the requirements was forwarded to his supervisor's superior who made the decision to fire Staub. In turn, Staub filed a grievance claiming the underlying reason for his disciplinary warning was that his supervisors were hostile toward his military obligations as a U.S. military reservist. Staub cited a history of work-scheduling conflicts requiring him to take leave or work additional shifts to fulfill his reservist obligations, as well as numerous derogatory comments concerning the military and his duties as a reservist.

This claim was brought under a "cat's paw" theory alleging that Proctor Hospital was liable for the animus of Staub's supervisors who did not make the actual decision to fire him, but did induce the decision maker to fire him based on the animosity they had towards Staub and his reservist status.[18] A jury found in favor of Staub and awarded him $57,740 in damages. On appeal, the Seventh Circuit determined that the cat's paw theory applies only to impute the animosity of a nondecision maker with "singular influence" over a decision maker and remanded to enter judgment in favor of Proctor Hospital.[19]

The U.S. Supreme Court granted certiorari and rejected

the circuit court's reasoning. It examined the question of under what circumstances an employer is liable for the unlawful intent of supervisors who cause or influence yet do not make the ultimate employment decision. In so doing, the Court considered both tort and agency law while focusing on the statutory term "motivating factor in the employer's action" found in the USERRA. Principles of tort law instruct that for intentional torts it is the intended consequences of an act, not simply the act, that determines the state of mind required for liability. Further, principles of agency law provide that both the supervisor and the ultimate decision maker, if both acting within the scope of their employment, are agents of the employer, and, thus, their wrongful conduct may be imputed to the employer. The Court concluded that the evidence suggested that a reasonable jury could have inferred that the actions of the supervisor were motivated by hostility toward Staub's military obligations and that these actions were causal factors underlying the ultimate decision to fire Staub.[20] The Court reversed the Seventh Circuit opinion and remanded for further proceedings to determine whether a new trial was warranted. This decision has the potential to affect liabilty issues in other federal acts, such as Title VII and the American with Disabilities Act (ADA), which has language similar to the USERRA.

Thompson v. North American Stainless, 131 S. Ct. 863 (2011)

This case continued the Supreme Court's broad interpretation of the antiretaliation provision within federal antidiscrimination law.[21] Eric Thompson, an engineer at North

American Stainless, a stainless steel manufacturer, was fired after his then-fiancée (now wife) filed a gender-discrimination complaint with the Equal Employment Opportunity Commission (EEOC). Thompson argued that because the company could not legally fire his fiancée in retaliation for her complaint, it fired him instead. At question in the case is whether Title VII—a federal antidiscrimination law—protects close family members and friends of a complaining employee or only the employee from retaliatory employer action.

The U.S. District Court for the Eastern District of Kentucky granted summary judgment to North American Stainless, finding that Title VII does not permit third-party retaliation claims. The Sixth Circuit Court of Appeals met en banc after a panel of the Sixth Circuit reversed the district court decision and affirmed the district court ruling.[22]

The case then was appealed to the U.S. Supreme Court, which advised that Title VII protects any employee who has made a charge under the act from employer discrimination.[23] Title VII also allows any person claiming to be aggrieved by an unlawful employment practice to file charges with the EEOC or even sue the employer if the EEOC declines to do so.[24] The Court then looked to the two issues presented by this case: First, if Thompson's firing by his employer was unlawful retaliation and, second, if so, if Thompson was entitled to relief under Title VII. The Court stated that if Thompson's statement of fact was true, then he was the subject of unlawful retaliation.[25] The Court went

on to say that Thompson was covered under Title VII due to the retaliation provision, which prohibits any employer action that "well might have dissuaded a reasonable worker from making or supporting a discrimination charge."[26] In regard to the issue of the proverbial "slippery slope" as to where protection against retaliation begins and ends and who is covered, the Court stated that no general rule should be made as any such rule would restrict the number of claimants unduly but that common sense should prevail because "the significance of any given act of retaliation will depend upon the particular circumstances."[27]

***Borough of Duryea, Pennsylvania v. Guarnieri,* 131 S. Ct. 2488 (2011)**

Embedded within the First Amendment is an individual's right to "petition the Government for a redress of grievances."[28] The parameters of this right were tested with the result being similar to what is seen in speech cases involving government employees.

Police Chief Charles J. Guarnieri was fired by the Borough of Duryea, Pennsylvania, in 2003 and subsequently filed a grievance to fight the firing. After arbitration, Chief Guarnieri was reinstated. Upon returning to his job, he found that the council had issued a number of directives limiting the tasks he could and could not do as chief. He then filed a second grievance, which resulted in the modification of the directives. He also sued the borough, alleging retaliation over his having filed the first grievance in 2003. Chief Guarnieri did so on the basis that the retaliation was a violation of his First Amendment right to petition. A jury found for Chief Guarnieri, and the borough appealed to the U.S. Third Circuit Court of Appeals, citing that only matters of public concern were protected under the First Amendment. The Third Circuit held that the First Amendment right to petition protects public employees concerning any manner, public or personal.[29]

The U.S. Supreme Court granted certiorari to determine the limitations of retaliation protection under the First Amendment right to petition. The Court long has held that for speech by a government employee to be protected under the First Amendment, it must address a matter of public concern.[30] Even if it addresses a matter of public concern before it is afforded protection, the Court must undergo a balancing-of-interests test between the government's need to manage its internal affairs and the interests of the individual in expressing matters of public concern to determine if the speech truly is protected. In this case involving the right to petition, the Court reasoned that a similar rubric should apply. The Court determined that to do otherwise in petition cases would undermine government efficiency and cause undue lawsuits in

federal courts dealing with internal management issues better left to internal resolution procedures, the states, or appropriate federal statutes that deal with employment issues.[31] The Court decided that a public employee's right to petition is a right to participate as a citizen in the democratic process, but not a right to transform everyday employment disputes into constitutional issues for federal litigation. For a public employee to bring a case involving the right to petition, there must be a matter of public concern.

Cases of Interest in the 2011-2012 Term

The U.S. Supreme Court has placed a number of cases of interest to law enforcement agencies on next year's docket. One of particular interest is *United States v. Jones*, where the court will decide whether the warrantless prolonged use of a global positioning system (GPS) tracking device to monitor a vehicle's movement on public streets violates the Fourth Amendment protection against unreasonable searches and seizures.[32] The second case of interest is *Messerschmitt v. Millender*, where the court will consider whether police officers are entitled to qualified immunity where they execute search warrants later deemed invalid.[33] In *Florence v. Board of Freeholders*, the Court has been asked to determine whether the Fourth Amendment permits strip searches by jailors for all offenses, including minor ones, without acting out of suspicion.[34] The final case of interest is *Howes v. Fields*, which involves Miranda and prison inmates.[35] The Court will determine whether a prisoner always is considered in custody for purposes of Miranda when the prisoner is isolated from the general prison population and questioned concerning conduct occurring outside the facility. ✦

Endnotes

[1] 768 N.W.2d 65 (Mich. 2009).
[2] 131 S. Ct. 1143, at 1168.
[3] *Id.* at 1150.
[4] 226 P.3d 1 (N.M. 2010).
[5] 129 S. Ct. 2527 (2009).
[6] 131 S. Ct. 2705, at 2716.
[7] *Brady v. Maryland*, 88 S. Ct. 1194 (1963).
[8] 109 S. Ct. 1197 (1989).
[9] 131 S. Ct. 1350, at 1361.
[10] 131 S. Ct. 1207, at 1210.
[11] *Id.* at 1220.
[12] 302 S.W.3d 649 (2010).
[13] *Id.* at 1863.
[14] 686 S.E.2d 135 (2009).
[15] 131 S. Ct. 2394, at 2404.
[16] 570 F.3d 834 (2009).
[17] 131 S. Ct. 1325, at 1331.
[18] "Cat's paw" comes from Jean de la Fontaine's *The Monkey and the Cat*, a fable involving a devious monkey who persuades an unsuspecting cat to take chestnuts from a fire. The cat burns its paws, while the monkey eats the chestnuts unscathed. Although it was the cat that was burned, the monkey induced the cat to take such action, making the cat an agent of the monkey's devious purpose. The cat's paw theory applied in the context of employment discrimination imputes liability to an employer for an adverse employment action taken by a nondiscriminating decision maker (the cat) induced into taking such action by the discrimination of another employee (the monkey).
[19] 560 F.3d 647 (2009).
[20] 131 S. Ct. 1186, at 1194.
[21] *See also Crawford v. Metropolitan Government of Nashville and Davidson County*, 129 S. Ct. 846 (2009); and *Burlington Northernand Santa Fe Railway Co. v. White*, 126 S. Ct. 2405 (2006).
[22] 567 F.3d 804 (2009).
[23] Title 42 U.S.C. § 2000e-3(a).
[24] *Id.* at 2000e-5(b), (f)(1).
[25] 131 S. Ct. 863, at 866.
[26] *Id.* at 869.
[27] *See Burlington N. & S.F.R. Comp. v. White*, 548 U.S. 59, at 69.
[28] First Amendment of the U.S. Constitution.
[29] 364 Fed. Appx. 749 (C.A.3 2010).
[30] *See Connick v. Myers*, 461 U.S. 138 (1983); and *City of San Diego v. Roe*, 125 S. Ct. 521 (2004).
[31] 131 S. Ct. 2488, at 2497.
[32] *U.S. v. Maynard*, 615 F.3d 544 (2010).
[33] *Millender v. County of Los Angeles*, 620 F.3d 1016 (2010).
[34] *Florence v. Board of Chosen Freeholders of County of Burlington*, 621 F.3d 296 (2010).
[35] *Fields v. Howes*, 617 F.3d 813 (2010).

Law enforcement officers of other than federal jurisdiction who are interested in this article should consult their legal advisors. Some police procedures ruled permissible under federal constitutional law are of questionable legality under state law or are not permitted at all.

Bulletin Notes

Law enforcement officers are challenged daily in the performance of their duties; they face each challenge freely and unselfishly while answering the call to duty. In certain instances, their actions warrant special attention from their respective departments. The *Bulletin* also wants to recognize those situations that transcend the normal rigors of the law enforcement profession.


Officer Hayes


Officer McCarthy


Officer McCluskey

Officers Matthew Hayes, Maryhelen McCarthy, and John McCluskey of the Newtown, Connecticut, Police Department responded to a call regarding a 9-year-old boy who had gone missing. The boy, who suffered from autism and was unable to verbalize, reportedly had ventured into a heavily wooded area close to his home. Upon arriving at the residence, all three officers began searching for the boy, with Officers McCarthy and McCluskey focusing their efforts toward a nearby stream. Officer McCluskey proceeded down a dirt trail that was located next to a pond; as he moved closer, he sighted the missing boy in the pond with water up to his chest, struggling to get out but unable to do so. Officers McCluskey and McCarthy immediately ran to the other side of the pond, climbed under a fence, and entered the water, saving the child from possibly drowning. Fortunately, the boy was uninjured and was reunited with his parents shortly thereafter.


Detective Howell

Officers of the Upper Sandusky, Ohio, Police Department responded to a call for three children who had fallen into a local river and could not be located. The officers found two of the children clinging to logs that were resting against a tree in the middle of the river; the third child had managed to make it to shore. The children were having difficulty holding onto the wet logs and were observed to slip back into the water on several occasions. Detective Tyler Howell, one of the officers at the scene, entered the river and swam over 30 feet against a very strong current in approximately 10 feet of water. Averting downed limbs and trees floating by, he reached the log jam the children were on and crawled along adjacent logs to reach them. He then secured the children in safety equipment, and they were pulled to shore by firemen, police officers, and lifeguards from the city pool.

Nominations for the ***Bulletin Notes*** should be based on either the rescue of one or more citizens or arrest(s) made at unusual risk to an officer's safety. Submissions should include a short write-up (maximum of 250 words), a separate photograph of each nominee, and a letter from the department's ranking officer endorsing the nomination. Submissions can be mailed to the Editor, *FBI Law Enforcement Bulletin*, FBI Academy, Quantico, VA 22135 or e-mailed to *leb@fbiacademy.edu*.

U.S. Department of Justice
Federal Bureau of Investigation
FBI Law Enforcement Bulletin
935 Pennsylvania Avenue, N.W.
Washington, DC 20535-0001

Periodicals
Postage and Fees Paid
Federal Bureau of Investigation
ISSN 0014-5688

Official Business
Penalty for Private Use $300

Patch Call

Various milestones in the history of Shreveport, Louisiana, are depicted on the patch of its police department. Flowing prominently at the bottom is the Red River, along which Shreveport was founded in 1833. The trees featured in the center represent the logging industry, and the American eagle symbolizes integrity and freedom. To the right is a profile of the Caddo Indian, who once occupied the local territory.

The city of Franklin, New Hampshire adopted its name in 1820 in honor of Benjamin Franklin. Another famous American statesman, Daniel Webster, is depicted on the patch of the Franklin Police Department. Webster was born in 1782 in a section of Franklin that was then part of Salisbury, New Hampshire. His birthplace has been preserved and is a state historic site.